IN THE CLAIMS

Please amend claims 5, 10-12 and 14 and add new claims 16-21, as shown:

1-4. (Canceled)

5. (Currently Amended) A method of protecting a host computer from unauthorized access by a client computer over a computer network, comprising the steps of:

installing a prover agent application on the client computer;

installing a verifier agent application on the host computer;

creating a trusted source application on the computer network to generate and publish encrypted values of a secret and product of first and second large prime numbers;

reading the encrypted values for the secret and product, by the prover and verifier from the trusted source;

decrypting the secret, by the prover and verifier;

decrypting the product, by the prover and verifier; ~~and~~

performing a plurality of verification dialog between the prover and verifier over the network, wherein the prover demonstrates knowledge of the secret and product without exposing the values of the secret and product, and wherein the client is denied access to a secure area of the host when the prover fails to demonstrate knowledge of the secret and product and granted access to the secure area when the client succeeds in demonstrating knowledge of the secret and product;

installing a first agent to be authenticated on a third computer on the network, the first agent having values for s, n and t, s being the secret, n being the product, and t being a size of an answer set;

installing a second agent on a fourth computer on the network, to authenticate the first agent, the second agent having values for s, n, and t;

generating r as a random number generated by the first agent;

calculating x by the first agent, r being raised to power of t modulus n;

sending x from the first agent to the second agent, over the network;

calculating b by the second agent, b being further defined as a member of set of integers from zero through t-1;

sending b from the second agent to the first agent, over the network;

calculating y by the first agent, y being a product of r*s raised to power of b;

sending y from the first agent to the second agent, over the network; and

determining authentication of the first agent, by determining equivalence of a first equation to a second equation, if y is not equal to zero, first equation is y^t mod n and second equation is (xv^b) mod n.

6. (Previously Presented) The method of claim 5, wherein the steps of decrypting the secret and product further utilize previous values of the secret and product as operators in the modulus inverse operations, to decrypt new values for the secret and the product.

7-9. (Cancelled)

10. (Currently Amended) The system of claim [[8]]5, the ~~requesting~~client computer comprising a cell phone.

11. (Currently Amended) The system of claim [[8]]5, the computer network comprising one or more of the Internet, a local area network, a communications link, and a wireless network.

12. (Currently Amended) The system of claim [[8]]5, the prover agent, verifier agent, first agent and second agent~~agents and prover agents~~ being respectively installed on ~~each of~~ the client computer, the host computer, the third computer and the fourth computer~~computers~~ through common software.

13. (Cancelled)

14. (Currently Amended) [[The]]A method of ~~claim 5,~~ protecting a host computer from unauthorized access by a client computer over a computer network, comprising the steps of:

installing a prover agent application on the client computer;

installing a verifier agent application on the host computer;

creating a trusted source application on the computer network to generate and publish encrypted values of a secret and product of first and second prime numbers;

reading the encrypted values for the secret and product, by the prover and verifier from the trusted source;

decrypting the secret, by the prover and verifier;

decrypting the product, by the prover and verifier;

performing a plurality of verification dialog between the prover and verifier over the network, wherein the prover demonstrates knowledge of the secret and product without exposing the values of the secret and product, and wherein the client is denied access to a secure area of the host when the prover fails to demonstrate knowledge of the secret and product and granted access to the secure area when the client succeeds in demonstrating knowledge of the secret and product;

wherein the prover has values for s, n and t, s being the secret, n being the product, and t being a size of an answer set and wherein the verifier having values for s, n and t; the verification dialog between the prover and verifier including:

generating r as a random number by the prover agent;

calculating x by the prover agent, r being raised to power of t modulus n;

sending x from the prover agent to the verifier agent, over the network;

calculating b by the verifier agent, b being further defined as a member of set of integers from zero through t-1;

sending b from the verifier agent to the prover agent, over the network;

calculating y by the prover agent, y being a product of r*s raised to power of b;

sending y from the prover agent to the verifier agent, over the network; and

determining authentication of the prover agent, by determining equivalence of a first equation to a second equation, if y is not equal to zero, the first equation is y^t mod n and the second equation is (xv^b) mod n.

15. (Previously Presented) A method of protecting a host computer from unauthorized access over a computer network, comprising the steps of:

installing a prover agent application on a client computer;

installing a verifier agent application on the host computer;

creating a trusted source application on the computer network to generate and publish encrypted values of a secret and product of first and second large prime numbers;

reading the encrypted values for the secret and product, by the prover and verifier from the trusted source;

decrypting the secret, by the prover and verifier;

decrypting the product, by the prover and verifier;

performing a plurality of verification dialog between the prover and verifier over the network, wherein the prover demonstrates knowledge of the secret and product without exposing the values of the secret and product, and wherein the client is denied access to a secure area of the host when the prover fails to demonstrate knowledge of the secret and product and granted access to the secure area when the client succeeds in demonstrating knowledge of the secret and product;

installing a first agent to be authenticated on a third computer on the network, the first agent having values for s, n and t, s being the secret, n being the product, and t being a size of an answer set;

installing a second agent on a fourth computer on the network, to authenticate the first agent, the second agent having values for s, n, and t;

generating r as a random number generated by the first agent;

calculating x by the first agent, r being raised to power of t modulus n;

sending x from the first agent to the second agent, over the network;

calculating b by the second agent, b being further defined as a member of set of integers from zero through t-1;

sending b from the second agent to the first agent, over the network;

calculating y by the first agent, y being a product of r*s raised to power of b;

sending y from the first agent to the second agent, over the network; and

determining authentication of the first agent, by determining equivalence of a first equation to a second equation, if y is not equal to zero, first equation is y^t mod n and second equation is (xv^b) mod n.

16. (New) The system of claim 14, the client computer comprising a cell phone.

17. (New) The system of claim 14, the computer network comprising one or more of the Internet, a local area network, a communications link, and a wireless network.

18. (New) The system of claim 14, the prover agent and the verifier agent being respectively installed on the client computer and the host computer through common software.

19. (New) The system of claim 15, the client computer comprising a cell phone.

20. (New) The system of claim 15, the computer network comprising one or more of the Internet, a local area network, a communications link, and a wireless network.

21. (New) The system of claim 15, the prover agent, verifier agent, first agent and second agent being respectively installed on the client computer, the host computer, the third computer and the fourth computer through common software.